Application of Information Theory, Lecture 9

Parallel Repetition of Interactive Arguments

Iftach Haitner

Tel Aviv University.

December 23, 2014

Part I

Interactive Proofs and Arguments

$\mathcal{NP}$ as a Non-interactive Proofs

Definition 1 ($\mathcal{NP}$)

$\mathcal{L} \in \mathcal{NP}$ iff $\exists$ and poly-time algorithm V such that:

- $\forall x \in \mathcal{L}$ there exists $w \in \{0,1\}^*$ s.t. $\mathsf{V}(x,w) = 1$
- $\mathsf{V}(x,w) = 0$ for every $x \notin \mathcal{L}$ and $w \in \{0,1\}^*$

Only $|x|$ counts for the running time of V.

$\mathcal{NP}$ as a Non-interactive Proofs

Definition 1 ($\mathcal{NP}$)

$\mathcal{L} \in \mathcal{NP}$ iff $\exists$ and poly-time algorithm V such that:

- $\forall x \in \mathcal{L}$ there exists $w \in \{0,1\}^*$ s.t. $\mathsf{V}(x, w) = 1$
- $\mathsf{V}(x, w) = 0$ for every $x \notin \mathcal{L}$ and $w \in \{0,1\}^*$

Only $|x|$ counts for the running time of V.

This proof system has

- Efficient verifier, efficient prover (given the witness)

$\mathcal{NP}$ as a Non-interactive Proofs

Definition 1 ($\mathcal{NP}$)

$\mathcal{L} \in \mathcal{NP}$ iff $\exists$ and poly-time algorithm V such that:

- $\forall x \in \mathcal{L}$ there exists $w \in \{0,1\}^*$ s.t. $\mathsf{V}(x,w) = 1$
- $\mathsf{V}(x,w) = 0$ for every $x \notin \mathcal{L}$ and $w \in \{0,1\}^*$

Only $|x|$ counts for the running time of V.

This proof system has

- Efficient verifier, efficient prover (given the witness)
- Soundness holds unconditionally

Interactive proofs/arguments

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P, V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P}, \mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*, \mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P,V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P},\mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*,\mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

- $\mathsf{IP} = \mathrm{PSPACE}$!

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P, V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P}, \mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*, \mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

- $\mathsf{IP} = \mathrm{PSPACE}$!
- The above protocol has completeness error $\frac{1}{3}$, and sourness error $\frac{1}{3}$

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P, V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P}, \mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*, \mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

- $\mathsf{IP} = \mathrm{PSPACE}$!
- The above protocol has completeness error $\frac{1}{3}$, and sourness error $\frac{1}{3}$
- We typically consider achieve (directly) perfect completeness.

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P, V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P}, \mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*, \mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

- $\mathrm{IP} = \mathrm{PSPACE}$!
- The above protocol has completeness error $\frac{1}{3}$, and sourness error $\frac{1}{3}$
- We typically consider achieve (directly) perfect completeness.
- Smaller “soundness error" achieved via repetition.

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P,V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P},\mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*,\mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

- $\mathsf{IP} = \mathrm{PSPACE}$!
- The above protocol has completeness error $\frac{1}{3}$, and sourness error $\frac{1}{3}$
- We typically consider achieve (directly) perfect completeness.
- Smaller “soundness error" achieved via repetition.
- Relaxation: interactive arguments [also known as, Computationally sound proofs]: soundness only guaranteed against efficient (PPT) provers.

Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficent prover.

Definition 2 (Interactive proof)

A protocol (P,V) is an interactive proof for $\mathcal{L}$, if V is a PPT and:

Completeness $\forall x \in \mathcal{L}$: $\Pr[(\mathsf{P},\mathsf{V})(x) = 1] \geq 2/3$.

Soundness $\forall x \notin \mathcal{L}$, and any algorithm P^*: $\Pr[(\mathsf{P}^*,\mathsf{V})(x) = 1] \leq 1/3$.

IP is the class of languages that have interactive proofs.

- $\mathsf{IP} = \mathrm{PSPACE}$!
- The above protocol has completeness error $\frac{1}{3}$, and sourness error $\frac{1}{3}$
- We typically consider achieve (directly) perfect completeness.
- Smaller “soundness error" achieved via repetition.
- Relaxation: interactive arguments [also known as, Computationally sound proofs]: soundness only guaranteed against efficient (PPT) provers.
- Games — no-input protocols.

Section 1

Interactive Proof for Graph Non-Isomorphism

Graph isomorphism

Π_m – the set of all permutations from $[m]$ to $[m]$

Definition 3 (graph isomorphism)

Graphs $G_0 = ([m], E_0)$ and $G_1 = ([m], E_1)$ are isomorphic, denoted $G_0 \equiv G_1$, if $\exists \pi \in \Pi_m$ such that
$(u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$.

Graph isomorphism

Π_m – the set of all permutations from $[m]$ to $[m]$

Definition 3 (graph isomorphism)

Graphs $G_0 = ([m], E_0)$ and $G_1 = ([m], E_1)$ are isomorphic, denoted $G_0 \equiv G_1$, if $\exists \pi \in \Pi_m$ such that
$(u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$.

- $\mathcal{GI} = \{(G_0, G_1) \colon G_0 \equiv G_1\} \in \mathcal{NP}$

Graph isomorphism

Π_m – the set of all permutations from $[m]$ to $[m]$

Definition 3 (graph isomorphism)

Graphs $\mathsf{G}_0 = ([m], E_0)$ and $\mathsf{G}_1 = ([m], E_1)$ are isomorphic, denoted $\mathsf{G}_0 \equiv \mathsf{G}_1$, if $\exists \pi \in \Pi_m$ such that
$(u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$.

- $\mathcal{GI} = \{(\mathsf{G}_0, \mathsf{G}_1) \colon \mathsf{G}_0 \equiv \mathsf{G}_1\} \in \mathcal{NP}$
- Does $\mathcal{GNI} = \{(\mathsf{G}_0, \mathsf{G}_1) \colon \mathsf{G}_0 \not\equiv \mathsf{G}_1\} \in \mathcal{NP}$?

Graph isomorphism

Π_m – the set of all permutations from $[m]$ to $[m]$

Definition 3 (graph isomorphism)

Graphs $G_0 = ([m], E_0)$ and $G_1 = ([m], E_1)$ are isomorphic, denoted $G_0 \equiv G_1$, if $\exists \pi \in \Pi_m$ such that
$(u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$.

- $\mathcal{GI} = \{(G_0, G_1) \colon G_0 \equiv G_1\} \in \mathcal{NP}$
- Does $\mathcal{GNI} = \{(G_0, G_1) \colon G_0 \not\equiv G_1\} \in \mathcal{NP}$?
- We will show a simple interactive proof for $\mathcal{GNI}$

Graph isomorphism

Π_m – the set of all permutations from $[m]$ to $[m]$

Definition 3 (graph isomorphism)

Graphs $\mathsf{G}_0 = ([m], E_0)$ and $\mathsf{G}_1 = ([m], E_1)$ are isomorphic, denoted $\mathsf{G}_0 \equiv \mathsf{G}_1$, if $\exists \pi \in \Pi_m$ such that
$(u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$.

- $\mathcal{GI} = \{(\mathsf{G}_0, \mathsf{G}_1) \colon \mathsf{G}_0 \equiv \mathsf{G}_1\} \in \mathcal{NP}$
- Does $\mathcal{GNI} = \{(\mathsf{G}_0, \mathsf{G}_1) \colon \mathsf{G}_0 \not\equiv \mathsf{G}_1\} \in \mathcal{NP}$?
- We will show a simple interactive proof for $\mathcal{GNI}$

Graph isomorphism

Π_m – the set of all permutations from $[m]$ to $[m]$

Definition 3 (graph isomorphism)

Graphs $G_0 = ([m], E_0)$ and $G_1 = ([m], E_1)$ are isomorphic, denoted $G_0 \equiv G_1$, if $\exists \pi \in \Pi_m$ such that
$(u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$.

- $\mathcal{GI} = \{(G_0, G_1) \colon G_0 \equiv G_1\} \in \mathcal{NP}$
- Does $\mathcal{GNI} = \{(G_0, G_1) \colon G_0 \not\equiv G_1\} \in \mathcal{NP}$?
- We will show a simple interactive proof for $\mathcal{GNI}$
  Idea: Beer tasting...

Interactive proof for $\mathcal{GNI}$

Protocol 4 $((\mathsf{P},\mathsf{V})(\mathsf{G}_0 = ([m], E_0), \mathsf{G}_1 = ([m], E_1)))$

1. V chooses $b \leftarrow \{0,1\}$ and $\pi \leftarrow \Pi_m$, and sends $\pi(E_b)$ to P.[a]
2. P send b' to V (tries to set $b' = b$).
3. V accepts iff $b' = b$.

[a] $\pi(E) = \{(\pi(u), \pi(v) \colon (u,v) \in E\}$.

Interactive proof for $\mathcal{GNI}$

Protocol 4 ($(\mathsf{P},\mathsf{V})(\mathsf{G}_0 = ([m], E_0), \mathsf{G}_1 = ([m], E_1))$)

1. V chooses $b \leftarrow \{0,1\}$ and $\pi \leftarrow \Pi_m$, and sends $\pi(E_b)$ to P.[a]
2. P send b' to V (tries to set $b' = b$).
3. V accepts iff $b' = b$.

[a] $\pi(E) = \{(\pi(u), \pi(v) \colon (u,v) \in E\}$.

Claim 5

The above protocol is IP for $\mathcal{GNI}$, with perfect completeness and soundness error $\frac{1}{2}$.

Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)

Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)

Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)
- $([m], \pi(E_i))$ is a random element in $[\mathrm{G}_i]$ — the equivalence class of G_i

Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)
- $([m], \pi(E_i))$ is a random element in $[\mathsf{G}_i]$ — the equivalence class of G_i

Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)
- $([m], \pi(E_i))$ is a random element in $[\mathsf{G}_i]$ — the equivalence class of G_i

Hence,

$\mathsf{G}_0 \equiv \mathsf{G}_1$: $\Pr[b' = b] \leq \frac{1}{2}$.

Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)
- $([m], \pi(E_i))$ is a random element in $[\mathsf{G}_i]$ — the equivalence class of G_i

Hence,

$\mathsf{G}_0 \equiv \mathsf{G}_1$: $\Pr[b' = b] \leq \frac{1}{2}$.

$\mathsf{G}_0 \not\equiv \mathsf{G}_1$: $\Pr[b' = b] = 1$ (i.e., P can, possibly inefficiently, extracted from $\pi(E_i)$)

□

Part II

Hardness Amplification

Hardness amplification

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.
- Two main approaches:

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - Parallel repetition: sometimes does not achieve optimal amplification rate and sometimes achieves nothing

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - Parallel repetition: sometimes does not achieve optimal amplification rate and sometimes achieves nothing
- How come parallel repetition might not work?

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by “amplifying the security” of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - Parallel repetition: sometimes does not achieve optimal amplification rate and sometimes achieves nothing
- How come parallel repetition might not work?

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - Parallel repetition: sometimes does not achieve optimal amplification rate and sometimes achieves nothing
- How come parallel repetition might not work? Example

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by "amplifying the security" of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - Parallel repetition: sometimes does not achieve optimal amplification rate and sometimes achieves nothing
- How come parallel repetition might not work? Example
- Parallel repetition does achieve optimal amplification rate for interactive proofs and public-coin interactive arguments

Hardness amplification

- In most settings we need very small soundness error (i.e., close to 0)
- Typically done by “amplifying the security” of an interactive proof/argument of large soundness error.
- Two main approaches:
  - Sequential repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - Parallel repetition: sometimes does not achieve optimal amplification rate and sometimes achieves nothing
- How come parallel repetition might not work? Example
- Parallel repetition does achieve optimal amplification rate for interactive proofs and public-coin interactive arguments
- Public-coin interactive proof/argument — in each round the verifier flips coins and sends them to the prover. To compute its output, the verifier applies some (fixed) function to the protocol’s transcript.

Hardness amplification, cont.

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.
- Typically, $s^{(k)} = s \cdot \mathrm{poly}(f(\varepsilon)/k)$

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.
- Typically, $s^{(k)} = s \cdot \mathrm{poly}(f(\varepsilon)/k)$
- If $f(\varepsilon) = \varepsilon^{\Omega(k)}$, the above is an exponential-rate amplification (and hence optimal)

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.
- Typically, $s^{(k)} = s \cdot \mathrm{poly}(f(\varepsilon)/k)$
- If $f(\varepsilon) = \varepsilon^{\Omega(k)}$, the above is an exponential-rate amplification (and hence optimal)
- If $f(\varepsilon) = \varepsilon^{\delta_1 \cdot k^{\delta_2}}$, the above is a weakly-exponential-rate amplification

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.
- Typically, $s^{(k)} = s \cdot \mathsf{poly}(f(\varepsilon)/k)$
- If $f(\varepsilon) = \varepsilon^{\Omega(k)}$, the above is an exponential-rate amplification (and hence optimal)
- If $f(\varepsilon) = \varepsilon^{\delta_1 \cdot k^{\delta_2}}$, the above is a weakly-exponential-rate amplification
- Why size?

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.
- Typically, $s^{(k)} = s \cdot \mathrm{poly}(f(\varepsilon)/k)$
- If $f(\varepsilon) = \varepsilon^{\Omega(k)}$, the above is an exponential-rate amplification (and hence optimal)
- If $f(\varepsilon) = \varepsilon^{\delta_1 \cdot k^{\delta_2}}$, the above is a weakly-exponential-rate amplification
- Why size?
- Concrete security

Hardness amplification, cont.

- Give a protocol $\pi = (\mathsf{P}, \mathsf{V})$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold parallel repetition of π: i.e., k parallel independent copies of π
- Assume $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size algorithm $\widetilde{\mathsf{P}}$, we would like to prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq f(\varepsilon)$ for any $s^{(k)}$-size algorithm $\widetilde{\mathsf{P}^{(k)}}$.
- Typically, $s^{(k)} = s \cdot \text{poly}(f(\varepsilon)/k)$
- If $f(\varepsilon) = \varepsilon^{\Omega(k)}$, the above is an exponential-rate amplification (and hence optimal)
- If $f(\varepsilon) = \varepsilon^{\delta_1 \cdot k^{\delta_2}}$, the above is a weakly-exponential-rate amplification
- Why size?
- Concrete security
- In the following we focus on games (no input protocols)

Section 2

Parallel repetition of public-coin interactive argument

Parallel repetition of public-coin interactive argument

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Proof plan: Let $\widetilde{\mathsf{P}^{(k)}}$ be $s^{(k)}$-size algorithm with $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3 s_{\mathsf{V}}}{\varepsilon^{(k)}}$-size $\widetilde{\mathsf{P}}$ with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq (\varepsilon^{(k)})^{4/k}$.

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Proof plan: Let $\widetilde{\mathsf{P}^{(k)}}$ be $s^{(k)}$-size algorithm with $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3 s_{\mathsf{V}}}{\varepsilon^{(k)}}$-size $\widetilde{\mathsf{P}}$ with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq (\varepsilon^{(k)})^{4/k}$.

- The $k/4$ in the exponent can be pushed to be almost k.

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Proof plan: Let $\widetilde{\mathsf{P}^{(k)}}$ be $s^{(k)}$-size algorithm with $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3 s_{\mathsf{V}}}{\varepsilon^{(k)}}$-size $\widetilde{\mathsf{P}}$ with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq (\varepsilon^{(k)})^{4/k}$.

- The $k/4$ in the exponent can be pushed to be almost k.
- Assume for simplicity that $\widetilde{\mathsf{P}^{(k)}}$ is deterministic

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Proof plan: Let $\widetilde{\mathsf{P}^{(k)}}$ be $s^{(k)}$-size algorithm with $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3 s_{\mathsf{V}}}{\varepsilon^{(k)}}$-size $\widetilde{\mathsf{P}}$ with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq (\varepsilon^{(k)})^{4/k}$.

- The $k/4$ in the exponent can be pushed to be almost k.
- Assume for simplicity that $\widetilde{\mathsf{P}^{(k)}}$ is deterministic
- Assume wlg. that V sends the first message in π and that in each round it samples and sends ℓ coins.

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Proof plan: Let $\widetilde{\mathsf{P}^{(k)}}$ be $s^{(k)}$-size algorithm with $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3 s_{\mathsf{V}}}{\varepsilon^{(k)}}$-size $\widetilde{\mathsf{P}}$ with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq (\varepsilon^{(k)})^{4/k}$.

- The $k/4$ in the exponent can be pushed to be almost k.
- Assume for simplicity that $\widetilde{\mathsf{P}^{(k)}}$ is deterministic
- Assume wlg. that V sends the first message in π and that in each round it samples and sends ℓ coins.
- We view the coins of $\mathsf{V}^{(k)}$ as a matrix $R \in \{0,1\}^{m \times (k\ell)}$, letting R_j denote the coins of the j'th round, and $R_{1,\ldots,j}$ the coins of the first j rounds.

Parallel repetition of public-coin interactive argument

Theorem 6

Let $\pi = (\mathsf{P}, \mathsf{V})$ be m-round, public-coin protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, then $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3 s_{\mathsf{V}}}$-size $\widetilde{\mathsf{P}^{(k)}}$, where s_{V} is V's size.

Proof plan: Let $\widetilde{\mathsf{P}^{(k)}}$ be $s^{(k)}$-size algorithm with $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3 s_{\mathsf{V}}}{\varepsilon^{(k)}}$-size $\widetilde{\mathsf{P}}$ with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq (\varepsilon^{(k)})^{4/k}$.

- The $k/4$ in the exponent can be pushed to be almost k.
- Assume for simplicity that $\widetilde{\mathsf{P}^{(k)}}$ is deterministic
- Assume wlg. that V sends the first message in π and that in each round it samples and sends ℓ coins.
- We view the coins of $\mathsf{V}^{(k)}$ as a matrix $R \in \{0,1\}^{m \times (k\ell)}$, letting R_j denote the coins of the j'th round, and $R_{1,\ldots,j}$ the coins of the first j rounds.
- Let $\mathbf{R} \sim \{0,1\}^{m \times (k\ell)}$

Algorithm $\widetilde{\mathsf{P}}$

Algorithm $\widetilde{\mathsf{P}}$

Let $q = k^2$.

Algorithm $\widetilde{\mathsf{P}}$

Let $q = k^2$.

Algorithm 7 ($\widetilde{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. Upon getting the j'th message r from V, do:
   - **2.1** Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \widetilde{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = r$.
   - **2.2** If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$:
     - **2.2.1** Set $\widetilde{R}_j = R_j$
     - **2.2.2** Send a_{j,i^*} back to V, for a_j being the j'th message $\widetilde{\mathsf{P}^{(k)}}$ send to $\mathsf{V}^{(k)}$ in $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R))$.

     Else, GOTO Line 2.1
   - **2.3** Abort if the overall number of sampling exceeds $\lceil qm/\varepsilon^{(k)} \rceil$.

Algorithm $\widetilde{\mathsf{P}}$

Let $q = k^2$.

Algorithm 7 ($\widetilde{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. Upon getting the j'th message r from V, do:

   2.1 Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \widetilde{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = r$.

   2.2 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$:

   - **2.2.1** Set $\widetilde{R}_j = R_j$
   - **2.2.2** Send a_{j,i^*} back to V, for a_j being the j'th message $\widetilde{\mathsf{P}^{(k)}}$ send to $\mathsf{V}^{(k)}$ in $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R))$.

   Else, GOTO Line 2.1

   2.3 Abort if the overall number of sampling exceeds $\lceil qm/\varepsilon^{(k)} \rceil$.

- Let $\widetilde{\mathsf{P}}'$ be the non aborting variant of $\widetilde{\mathsf{P}}'$, let $\widetilde{\mathbf{R}}$ and $\widetilde{\mathbf{N}}$ be the value of $\widetilde{R}$ and $\#$ of samples done in a random execution of $(\widetilde{\mathsf{P}}', \mathsf{V}^{(k)})$.

Algorithm $\widetilde{\mathsf{P}}$

Let $q = k^2$.

Algorithm 7 ($\widetilde{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. Upon getting the j'th message r from V, do:
   - **2.1** Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \widetilde{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = r$.
   - **2.2** If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$:
     - **2.2.1** Set $\widetilde{R}_j = R_j$
     - **2.2.2** Send a_{j,i^*} back to V, for a_j being the j'th message $\widetilde{\mathsf{P}^{(k)}}$ send to $\mathsf{V}^{(k)}$ in $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R))$.

     Else, GOTO Line 2.1
   - **2.3** Abort if the overall number of sampling exceeds $\lceil qm/\varepsilon^{(k)} \rceil$.

- Let $\widetilde{\mathsf{P}}'$ be the non aborting variant of $\widetilde{\mathsf{P}}'$, let $\widetilde{\mathbf{R}}$ and $\widetilde{\mathbf{N}}$ be the value of $\widetilde{R}$ and $\#$ of samples done in a random execution of $(\widetilde{\mathsf{P}}', \mathsf{V}^{(k)})$.
- $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \geq \Pr\left[\mathrm{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) := (\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\widetilde{\mathbf{R}})) = 1^k \wedge \widetilde{\mathbf{N}} \leq qm/\varepsilon^{(k)}\right]$.

Ideal "attacker"

Ideal "attacker"

Experiment 8 ($\hat{\mathrm{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathrm{P}^{(k)}}, \mathrm{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

Ideal "attacker"

Experiment 8 ($\hat{\mathsf{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

- Let $\hat{\mathbf{R}}$ be the value of $\hat{R}$ in the end of a random execution of $\hat{\mathsf{P}}$.

Ideal "attacker"

Experiment 8 ($\hat{\mathsf{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

- Let $\hat{\mathbf{R}}$ be the value of $\hat{R}$ in the end of a random execution of $\hat{\mathsf{P}}$.
- $\hat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$

Ideal "attacker"

Experiment 8 ($\hat{\mathsf{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

- Let $\hat{\mathbf{R}}$ be the value of $\hat{R}$ in the end of a random execution of $\hat{\mathsf{P}}$.
- $\hat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- In particular, $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\hat{\mathbf{R}}) = 1^k\right] = 1$

Ideal "attacker"

Experiment 8 ($\hat{\mathsf{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

- Let $\hat{\mathbf{R}}$ be the value of $\hat{R}$ in the end of a random execution of $\hat{\mathsf{P}}$.
- $\hat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- In particular, $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\hat{\mathbf{R}}) = 1^k\right] = 1$
- Let $\hat{\mathbf{N}}$ be $\#$ of samples done in $\hat{\mathbf{R}}$.

Ideal "attacker"

Experiment 8 ($\hat{\mathsf{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

- Let $\hat{\mathbf{R}}$ be the value of $\hat{R}$ in the end of a random execution of $\hat{\mathsf{P}}$.
- $\hat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- In particular, $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\hat{\mathbf{R}}) = 1^k\right] = 1$
- Let $\hat{\mathbf{N}}$ be $\#$ of samples done in $\hat{\mathbf{R}}$.

Ideal "attacker"

Experiment 8 ($\hat{\mathsf{P}}$)

For $j = 1$ to m:

1. Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned that $R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}$.
2. If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\hat{R}_j = R_j$. Else, GOTO Line 1.

- Let $\hat{\mathbf{R}}$ be the value of $\hat{R}$ in the end of a random execution of $\hat{\mathsf{P}}$.
- $\hat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- In particular, $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\hat{\mathbf{R}}) = 1^k\right] = 1$
- Let $\hat{\mathbf{N}}$ be $\#$ of samples done in $\hat{\mathbf{R}}$.

Lemma 9

$\Pr\left[\hat{\boldsymbol{N}} \leq qm/\varepsilon^{(k)}\right] \geq 1 - \frac{1}{q}$

Proving Lemma 9

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$
  (letting $X^j = (X_1, \ldots, X_j)$)

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$
  (letting $X^j = (X_1, \ldots, X_j)$)
- Conditioned on $Y^j = \mathbf{y} = (y_1, \ldots, y_j)$, the expected $\#$ of samples done in $(j+1)$'th round of $\widehat{\mathsf{P}}$ is $\frac{1}{v(\mathbf{y})}$.

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$
  (letting $X^j = (X_1, \ldots, X_j)$)
- Conditioned on $Y^j = \mathbf{y} = (y_1, \ldots, y_j)$, the expected $\#$ of samples done in $(j+1)$'th round of $\widehat{\mathsf{P}}$ is $\frac{1}{v(\mathbf{y})}$.
- We prove Lemma 9 showing that $\mathrm{E}\left[\frac{1}{v(Y^j)}\right] \leq \frac{1}{\varepsilon^{(k)}}$ for every $j \in \{0, \ldots, m-1\}$

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$
  (letting $X^j = (X_1, \ldots, X_j)$)
- Conditioned on $Y^j = \mathbf{y} = (y_1, \ldots, y_j)$, the expected $\#$ of samples done in $(j+1)$'th round of $\widehat{\mathsf{P}}$ is $\frac{1}{v(\mathbf{y})}$.
- We prove Lemma 9 showing that $\mathrm{E}\left[\frac{1}{v(Y^j)}\right] \leq \frac{1}{\varepsilon^{(k)}}$ for every $j \in \{0, \ldots, m-1\}$

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$ (letting $X^j = (X_1, \ldots, X_j)$)
- Conditioned on $Y^j = \mathbf{y} = (y_1, \ldots, y_j)$, the expected $\#$ of samples done in $(j+1)$'th round of $\widehat{\mathsf{P}}$ is $\frac{1}{v(\mathbf{y})}$.
- We prove Lemma 9 showing that $\mathrm{E}\left[\frac{1}{v(Y^j)}\right] \leq \frac{1}{\varepsilon^{(k)}}$ for every $j \in \{0, \ldots, m-1\}$

Claim 10

For $j \in \{0, \ldots, m-1\}$ and $\mathbf{y} \in \mathrm{Supp}(Y^j)$ it holds that $\Pr_{Y^j}[\mathbf{y}] = \Pr_{X^j}[\mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}}$

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$
  (letting $X^j = (X_1, \ldots, X_j)$)
- Conditioned on $Y^j = \mathbf{y} = (y_1, \ldots, y_j)$, the expected $\#$ of samples done in $(j+1)$'th round of $\widehat{\mathsf{P}}$ is $\frac{1}{v(\mathbf{y})}$.
- We prove Lemma 9 showing that $\mathrm{E}\left[\frac{1}{v(Y^j)}\right] \leq \frac{1}{\varepsilon^{(k)}}$ for every $j \in \{0, \ldots, m-1\}$

Claim 10

For $j \in \{0, \ldots, m-1\}$ and $\mathbf{y} \in \mathrm{Supp}(Y^j)$ it holds that $\Pr_{Y^j}[\mathbf{y}] = \Pr_{X^j}[\mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}}$

Hence, $\mathrm{E}_{Y^j}\left[\frac{1}{v(Y^j)}\right] = \sum_{\mathbf{y} \in \mathrm{Supp}(Y^j)} \Pr[Y^j = \mathbf{y}] \cdot \frac{1}{v(\mathbf{y})}$

Proving Lemma 9

- Let $(X_1, \ldots, X_m) = \mathbf{R}$ and $(Y_1, \ldots, Y_m) = \widehat{\mathbf{R}}$
- $v(\mathbf{y} = (y_1, \ldots, y_j)) := \Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(X^m)) = 1^k \mid X^j = \mathbf{y}\right]$
  (letting $X^j = (X_1, \ldots, X_j)$)
- Conditioned on $Y^j = \mathbf{y} = (y_1, \ldots, y_j)$, the expected $\#$ of samples done in $(j+1)$'th round of $\widehat{\mathsf{P}}$ is $\frac{1}{v(\mathbf{y})}$.
- We prove Lemma 9 showing that $\mathrm{E}\left[\frac{1}{v(Y^j)}\right] \le \frac{1}{\varepsilon^{(k)}}$ for every $j \in \{0, \ldots, m-1\}$

Claim 10

For $j \in \{0, \ldots, m-1\}$ and $\mathbf{y} \in \mathrm{Supp}(Y^j)$ it holds that $\Pr_{Y^j}[\mathbf{y}] = \Pr_{X^j}[\mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}}$

Hence, $\mathrm{E}_{Y^j}\left[\frac{1}{v(Y^j)}\right] = \sum_{\mathbf{y} \in \mathrm{Supp}(Y^j)} \Pr[Y^j = \mathbf{y}] \cdot \frac{1}{v(\mathbf{y})}$
$= \sum_{\mathbf{y}} \Pr[X^j = \mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}} \cdot \frac{1}{v(\mathbf{y})} = \frac{1}{\varepsilon^{(k)}} \cdot \sum_{\mathbf{y} \in \mathrm{Supp}(Y^j)} \Pr[X^j = \mathbf{y}] \le \frac{1}{\varepsilon^{(k)}}$. $\square$

Proving Claim 10

Proving Claim 10

Note that

$$\Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j] = \sum_{\ell=1}^{\infty}(1-v(\mathbf{y}_{1\ldots,j-1}))^{\ell-1}\cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j]\cdot v(\mathbf{y}) \tag{1}$$

$$= \frac{1}{v(\mathbf{y}_{1\ldots,j-1})}\cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j]\cdot v(\mathbf{y})$$

Proving Claim 10

Note that

$$\Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] = \sum_{\ell=1}^{\infty}(1 - v(\mathbf{y}_{1,\dots,j-1}))^{\ell-1} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \cdot v(\mathbf{y}) \qquad (1)$$

$$= \frac{1}{v(\mathbf{y}_{1,\dots,j-1})} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \cdot v(\mathbf{y})$$

The proof proceeds by induction on j.

Proving Claim 10

Note that

$$\Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j] = \sum_{\ell=1}^{\infty}(1 - v(\mathbf{y}_{1\ldots,j-1}))^{\ell-1} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j] \cdot v(\mathbf{y}) \tag{1}$$
$$= \frac{1}{v(\mathbf{y}_{1\ldots,j-1})} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j] \cdot v(\mathbf{y})$$

The proof proceeds by induction on j.

$\Pr_{Y^j}[\mathbf{y}] = \Pr_{Y^{j-1}}\left[\mathbf{y}_{1\ldots,j-1}\right] \cdot \Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1\ldots,j-1}}[y_j]$

Proving Claim 10

Note that

$$\Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] = \sum_{\ell=1}^{\infty}(1 - v(\mathbf{y}_{1,\dots,j-1}))^{\ell-1} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \cdot v(\mathbf{y}) \qquad (1)$$

$$= \frac{1}{v(\mathbf{y}_{1,\dots,j-1})} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \cdot v(\mathbf{y})$$

The proof proceeds by induction on j.

$$\Pr_{Y^j}[\mathbf{y}] = \Pr_{Y^{j-1}}\left[\mathbf{y}_{1,\dots,j-1}\right] \cdot \Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j]$$

$$= \Pr_{X^{j-1}}\left[\mathbf{y}_{1,\dots,j-1}\right] \cdot \frac{v(\mathbf{y}_{1,\dots,j-1})}{\varepsilon^{(k)}} \cdot \Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \qquad \text{(i.h.)}$$

Proving Claim 10

Note that

$$\Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] = \sum_{\ell=1}^{\infty}(1 - v(\mathbf{y}_{1\dots,j-1}))^{\ell-1} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \cdot v(\mathbf{y}) \qquad (1)$$

$$= \frac{1}{v(\mathbf{y}_{1\dots,j-1})} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \cdot v(\mathbf{y})$$

The proof proceeds by induction on j.

$$\Pr_{Y^j}[\mathbf{y}] = \Pr_{Y^{j-1}}\left[\mathbf{y}_{1\dots,j-1}\right] \cdot \Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j]$$

$$= \Pr_{X^{j-1}}\left[\mathbf{y}_{1\dots,j-1}\right] \cdot \frac{v(\mathbf{y}_{1\dots,j-1})}{\varepsilon^{(k)}} \cdot \Pr_{Y_j|Y^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \qquad \text{(i.h.)}$$

$$= \Pr_{X^{j-1}}\left[\mathbf{y}_{1\dots,j-1}\right] \cdot \frac{v(\mathbf{y}_{1\dots,j-1})}{\varepsilon^{(k)}} \cdot \frac{v(\mathbf{y})}{v(\mathbf{y}_{1\dots,j-1})} \cdot \Pr_{X_j|X^{j-1}=\mathbf{y}_{1,\dots,j-1}}[y_j] \qquad \text{(Eq. (1))}$$

Proving Claim 10

Note that

$$\Pr_{Y_j | Y^{j-1} = \mathbf{y}_{1,\dots,j-1}} [y_j] = \sum_{\ell=1}^{\infty} (1 - v(\mathbf{y}_{1,\dots,j-1}))^{\ell-1} \cdot \Pr_{X_j | X^{j-1} = \mathbf{y}_{1,\dots,j-1}} [y_j] \cdot v(\mathbf{y}) \qquad (1)$$
$$= \frac{1}{v(\mathbf{y}_{1,\dots,j-1})} \cdot \Pr_{X_j | X^{j-1} = \mathbf{y}_{1,\dots,j-1}} [y_j] \cdot v(\mathbf{y})$$

The proof proceeds by induction on j.

$$\Pr_{Y^j} [\mathbf{y}] = \Pr_{Y^{j-1}} \left[\mathbf{y}_{1,\dots,j-1}\right] \cdot \Pr_{Y_j | Y^{j-1} = \mathbf{y}_{1,\dots,j-1}} [y_j]$$
$$= \Pr_{X^{j-1}} \left[\mathbf{y}_{1,\dots,j-1}\right] \cdot \frac{v(\mathbf{y}_{1,\dots,j-1})}{\varepsilon^{(k)}} \cdot \Pr_{Y_j | Y^{j-1} = \mathbf{y}_{1,\dots,j-1}} [y_j] \qquad \text{(i.h.)}$$
$$= \Pr_{X^{j-1}} \left[\mathbf{y}_{1,\dots,j-1}\right] \cdot \frac{v(\mathbf{y}_{1,\dots,j-1})}{\varepsilon^{(k)}} \cdot \frac{v(\mathbf{y})}{v(\mathbf{y}_{1,\dots,j-1})} \cdot \Pr_{X_j | X^{j-1} = \mathbf{y}_{1,\dots,j-1}} [y_j] \qquad \text{(Eq. (1))}$$
$$= \Pr_{X^j} [\mathbf{y}] \cdot \frac{v(\mathbf{y})}{\varepsilon^{(k)}}.$$

Ideal "attacker", variant

Ideal "attacker", variant

Experiment 11 ($\widehat{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. For for $j = 1$ to m:

   2.1 Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$.

   2.2 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_{j,i^*} = R_{j,i^*}$. Else, GOTO Line 2.1.

   2.3 Let $R \leftarrow \{0,1\}^{m\times\ell}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = \widehat{R}_{j,i^*}$.

   2.4 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_j = R_j$. Else, GOTO Line 2.3.

Ideal "attacker", variant

Experiment 11 ($\widehat{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. For for $j = 1$ to m:

   2.1 Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned on $R_{1,\dots,j-1} = \widehat{R}_{1,\dots,j-1}$.

   2.2 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_{j,i^*} = R_{j,i^*}$. Else, GOTO Line 2.1.

   2.3 Let $R \leftarrow \{0,1\}^{m \times \ell}$, conditioned on $R_{1,\dots,j-1} = \widehat{R}_{1,\dots,j-1}$ and $R_{j,i^*} = \widehat{R}_{j,i^*}$.

   2.4 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_j = R_j$. Else, GOTO Line 2.3.

- Let $\widehat{\mathbf{R}}$ be the final value of $\widehat{R}$ in $\widehat{\mathsf{P}}$.

Ideal "attacker", variant

Experiment 11 ($\widehat{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. For for $j = 1$ to m:
   - **2.1** Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$.
   - **2.2** If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_{j,i^*} = R_{j,i^*}$. Else, GOTO Line 2.1.
   - **2.3** Let $R \leftarrow \{0,1\}^{m\times\ell}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = \widehat{R}_{j,i^*}$.
   - **2.4** If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_j = R_j$. Else, GOTO Line 2.3.

- Let $\widehat{\mathbf{R}}$ be the final value of $\widehat{R}$ in $\widehat{\mathsf{P}}$.
- $\widehat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$

Ideal "attacker", variant

Experiment 11 ($\widehat{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. For for $j = 1$ to m:

   2.1 Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned on $R_{1,\dots,j-1} = \widehat{R}_{1,\dots,j-1}$.

   2.2 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_{j,i^*} = R_{j,i^*}$. Else, GOTO Line 2.1.

   2.3 Let $R \leftarrow \{0,1\}^{m\times\ell}$, conditioned on $R_{1,\dots,j-1} = \widehat{R}_{1,\dots,j-1}$ and $R_{j,i^*} = \widehat{R}_{j,i^*}$.

   2.4 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_j = R_j$. Else, GOTO Line 2.3.

- Let $\widehat{\mathbf{R}}$ be the final value of $\widehat{R}$ in $\widehat{\mathsf{P}}$.
- $\widehat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- Let $\widehat{\mathbf{N}}$ be the $\#$ of Step-2.3-samples done in $\widehat{\mathsf{P}}$.

Ideal "attacker", variant

Experiment 11 ($\widehat{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. For for $j = 1$ to m:

    2.1 Let $R \leftarrow \{0,1\}^{m\times(k\ell)}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$.

    2.2 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_{j,i^*} = R_{j,i^*}$. Else, GOTO Line 2.1.

    2.3 Let $R \leftarrow \{0,1\}^{m\times\ell}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = \widehat{R}_{j,i^*}$.

    2.4 If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_j = R_j$. Else, GOTO Line 2.3.

- Let $\widehat{\mathbf{R}}$ be the final value of $\widehat{R}$ in $\widehat{\mathsf{P}}$.
- $\widehat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}},\mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- Let $\widehat{\mathbf{N}}$ be the $\#$ of Step-2.3-samples done in $\widehat{\mathsf{P}}$.

Ideal "attacker", variant

Experiment 11 ($\widehat{\mathsf{P}}$)

1. Let $i^* \leftarrow [k]$.
2. For for $j = 1$ to m:
   - **2.1** Let $R \leftarrow \{0,1\}^{m \times (k\ell)}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$.
   - **2.2** If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_{j,i^*} = R_{j,i^*}$. Else, GOTO Line 2.1.
   - **2.3** Let $R \leftarrow \{0,1\}^{m \times \ell}$, conditioned on $R_{1,\ldots,j-1} = \widehat{R}_{1,\ldots,j-1}$ and $R_{j,i^*} = \widehat{R}_{j,i^*}$.
   - **2.4** If $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(R)) = 1^k$, set $\widehat{R}_j = R_j$. Else, GOTO Line 2.3.

- Let $\widehat{\mathbf{R}}$ be the final value of $\widehat{R}$ in $\widehat{\mathsf{P}}$.
- $\widehat{\mathbf{R}} \sim \mathbf{R}|_{(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k}$
- Let $\widehat{\mathbf{N}}$ be the $\#$ of Step-2.3-samples done in $\widehat{\mathsf{P}}$.

Lemma 12

$\Pr\left[\text{win}(\widehat{\boldsymbol{R}}, \widehat{\boldsymbol{N}})\right] \geq 1 - \frac{1}{q}$

From ideal to real

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- Hence, $D(\mathrm{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}}) || \mathrm{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})) \leq D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- Hence, $D(\text{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}}) || \text{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})) \leq D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$
- Claim 12 $\implies \alpha := \Pr[\text{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}})] \geq 1 - \frac{1}{q}$, and let $\beta := \Pr[\text{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})]$.

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- Hence, $D(\mathrm{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}}) || \mathrm{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})) \leq D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$
- Claim 12 $\implies \alpha := \Pr[\mathrm{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}})] \geq 1 - \frac{1}{q}$, and let $\beta := \Pr[\mathrm{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})]$.
- By data-processing inequality, $\alpha \cdot \log \frac{\alpha}{\beta} + (1-\alpha) \log(1-\alpha) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- Hence, $D(\text{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}}) || \text{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})) \leq D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$
- Claim 12 $\implies \alpha := \Pr[\text{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}})] \geq 1 - \frac{1}{q}$, and let $\beta := \Pr[\text{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})]$.
- By data-processing inequality, $\alpha \cdot \log \frac{\alpha}{\beta} + (1-\alpha) \log(1-\alpha) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$

  $\implies \beta \geq 2^{\log \alpha + \frac{1-\alpha}{\alpha} \log(1-\alpha) + \frac{1}{\alpha k} \log \varepsilon^{(k)}}$

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i \in [k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i \in [k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}, \mathsf{V}^{(k)}}(\mathbf{R})) = 1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- Hence, $D(\operatorname{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}}) || \operatorname{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})) \leq D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$
- Claim 12 $\implies \alpha := \Pr[\operatorname{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}})] \geq 1 - \frac{1}{q}$, and let $\beta := \Pr[\operatorname{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})]$.
- By data-processing inequality, $\alpha \cdot \log \frac{\alpha}{\beta} + (1-\alpha) \log(1-\alpha) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$

  $\implies \beta \geq 2^{\log \alpha + \frac{1-\alpha}{\alpha} \log(1-\alpha) + \frac{1}{\alpha k} \log \varepsilon^{(k)}}$
- Recalling $q = k^2$, $\alpha \geq 2^{-\frac{2}{q}} \geq 2^{-\frac{1}{k}}$ and $\frac{1-\alpha}{\alpha} \log(1-\alpha) \geq -\frac{4 \log k}{k^2} \geq -\frac{1}{k}$

From ideal to real

Let $\widetilde{\mathbf{R}}_i = \widetilde{\mathbf{R}}|_{i^*=i}$ and $\widehat{\mathbf{R}}_i := \widehat{\mathbf{R}}|_{i^*=i} \quad (= \widehat{\mathbf{R}})$.

Claim 13

$D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq \frac{1}{k} \sum_{i\in[k]} D(\widehat{\mathbf{R}}_i || \widetilde{\mathbf{R}}_i)$.

Claim 14

$\sum_{i\in[k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) \leq D(\widehat{\mathbf{R}} || \mathbf{R})$.

- Thm. 7 in Lecture 7 $\implies D(\widehat{\mathbf{R}} || \mathbf{R}) \leq \log \frac{1}{\Pr[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R}))=1^k]} = \log \frac{1}{\varepsilon^{(k)}}$
- Hence, $D(\mathrm{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}}) || \mathrm{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})) \leq D(\widehat{\mathbf{R}}, \widehat{\mathbf{N}} || \widetilde{\mathbf{R}}, \widetilde{\mathbf{N}}) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$
- Claim 12 $\implies \alpha := \Pr[\mathrm{win}(\widehat{\mathbf{R}}, \widehat{\mathbf{N}})] \geq 1 - \frac{1}{q}$, and let $\beta := \Pr[\mathrm{win}(\widetilde{\mathbf{R}}, \widetilde{\mathbf{N}})]$.
- By data-processing inequality, $\alpha \cdot \log \frac{\alpha}{\beta} + (1-\alpha) \log(1-\alpha) \leq -\frac{1}{k} \cdot \log \varepsilon^{(k)}$

  $\implies \beta \geq 2^{\log \alpha + \frac{1-\alpha}{\alpha} \log(1-\alpha) + \frac{1}{\alpha k} \log \varepsilon^{(k)}}$
- Recalling $q = k^2$, $\alpha \geq 2^{-\frac{2}{q}} \geq 2^{-\frac{1}{k}}$ and $\frac{1-\alpha}{\alpha} \log(1-\alpha) \geq -\frac{4 \log k}{k^2} \geq -\frac{1}{k}$
- We conclude that $\beta \geq 2^{\frac{4}{k} \log \varepsilon^{(k)}} = \sqrt[k/4]{\varepsilon^{(k)}}$.□

Proving Claim 13

Proving Claim 13

HW...

Proving Claim 14

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ *be iids, let* W *be an event, and let*
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W || D_i) \leq D(Z|_W || Z)$.

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ be iids, let W be an event, and let
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W||D_i) \leq D(Z|_W||Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}}||\widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W||\widetilde{\mathbf{R}}_i) \leq D(\mathbf{R}|_W||\mathbf{R}) = D(\widehat{\mathbf{R}}||\mathbf{R})$. $\square$

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ be iids, let W be an event, and let
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W || D_i) \le D(Z|_W || Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathsf{P}^{(k)}, \mathsf{V}^{(k)}}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W || \widetilde{\mathbf{R}}_i) \le D(\mathbf{R}|_W || \mathbf{R}) = D(\widehat{\mathbf{R}} || \mathbf{R})$. $\square$

Proof: (of Lemma 15) We prove for $m = k = 2$.

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ be iids, let W be an event, and let
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W || D_i) \leq D(Z|_W || Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W || \widetilde{\mathbf{R}}_i) \leq D(\mathbf{R}|_W || \mathbf{R}) = D(\widehat{\mathbf{R}} || \mathbf{R})$. $\square$

Proof: (of Lemma 15) We prove for $m = k = 2$.

- Let $X = Z_1$ and $Y = Z_2$

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ be iids, let W be an event, and let
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W || D_i) \le D(Z|_W || Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W || \widetilde{\mathbf{R}}_i) \le D(\mathbf{R}|_W || \mathbf{R}) = D(\widehat{\mathbf{R}} || \mathbf{R})$. $\square$

Proof: (of Lemma 15) We prove for $m = k = 2$.

- Let $X = Z_1$ and $Y = Z_2$
- $U(x_1, x_2, y_1, y_2) := \Pr_{(X,Y)}\left[(x_1, x_2, y_1, y_2)\right]$

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ be iids, let W be an event, and let
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \land Z_{j,i} = z_{i,j} \land W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W || D_i) \leq D(Z|_W || Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathsf{P}^{(k)}, \mathsf{V}^{(k)}}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}} || \widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W || \widetilde{\mathbf{R}}_i) \leq D(\mathbf{R}|_W || \mathbf{R}) = D(\widehat{\mathbf{R}} || \mathbf{R})$. $\square$

Proof: (of Lemma 15) We prove for $m = k = 2$.

- Let $X = Z_1$ and $Y = Z_2$
- $U(x_1, x_2, y_1, y_2) := \Pr_{(X,Y)}\left[(x_1, x_2, y_1, y_2)\right]$
- $C(x_1, x_2, y_1, y_1) := \Pr_{(X,Y)|_W}\left[(x_1, x_2, y_1, y_2)\right]$

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ *be iids, let* W *be an event, and let*
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W||D_i) \leq D(Z|_W||Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathrm{P}^{(k)}, \mathrm{V}^{(k)}}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}}||\widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W||\widetilde{\mathbf{R}}_i) \leq D(\mathbf{R}|_W||\mathbf{R}) = D(\widehat{\mathbf{R}}||\mathbf{R})$. □

Proof: (of Lemma 15) We prove for $m = k = 2$.

- Let $X = Z_1$ and $Y = Z_2$
- $U(x_1, x_2, y_1, y_2) := \Pr_{(X,Y)}\left[(x_1, x_2, y_1, y_2)\right]$
- $C(x_1, x_2, y_1, y_1) := \Pr_{(X,Y)|_W}\left[(x_1, x_2, y_1, y_2)\right]$
- $Q(x_1, x_2, y_1, y_1) := \Pr\left[X_1 = x_1 | W\right] \cdot \Pr\left[X_2 = x_2 | W\right] \cdot$
  $\Pr\left[Y_1 = y_1 | W, X = (x_1, x_2)\right] \cdot \Pr\left[Y_2 = y_2 | W, X = (x_1, x_2)\right]$

Proving Claim 14

Lemma 15

Let $Z = \{Z_{ij}\}_{(i,j)\in[k]\times[m]}$ *be iids, let* W *be an event, and let*
$D_i(z) := \prod_{j=1}^{m} \Pr\left[Z_{j,i} = z_{i,j}\right] \cdot \Pr\left[Z_{j,-i} = z_{i,j-1} | Z_{1,\ldots,j-1} = z_{1,\ldots,j-1} \wedge Z_{j,i} = z_{i,j} \wedge W\right]$.
Then $\sum_{i=1}^{k} D(Z|_W || D_i) \leq D(Z|_W || Z)$.

Letting $Z = \mathbf{R}$ and W be the event $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}(\mathbf{R})) = 1^k$, Lemma 15 yields that $\sum_{i\in[k]} D(\widehat{\mathbf{R}}||\widetilde{\mathbf{R}}_i) = \sum_{i\in[k]} D(\mathbf{R}|_W||\widetilde{\mathbf{R}}_i) \leq D(\mathbf{R}|_W||\mathbf{R}) = D(\widehat{\mathbf{R}}||\mathbf{R})$. □

Proof: (of Lemma 15) We prove for $m = k = 2$.

- Let $X = Z_1$ and $Y = Z_2$
- $U(x_1, x_2, y_1, y_2) := \Pr_{(X,Y)}\left[(x_1, x_2, y_1, y_2)\right]$
- $C(x_1, x_2, y_1, y_1) := \Pr_{(X,Y)|_W}\left[(x_1, x_2, y_1, y_2)\right]$
- $Q(x_1, x_2, y_1, y_1) := \Pr\left[X_1 = x_1 | W\right] \cdot \Pr\left[X_2 = x_2 | W\right] \cdot \Pr\left[Y_1 = y_1 | W, X = (x_1, x_2)\right] \cdot \Pr\left[Y_2 = y_2 | W, X = (x_1, x_2)\right]$
- We write $\frac{C(x_1,x_2,y_1,y_1)}{U(x_1,x_2,y_1,y_1)} = \frac{\Pr[X_1=x_1|W]\cdot\Pr[Y_1=y_1|W,X=(x_1,x_2)]}{\Pr[X_1=x_1]\cdot\Pr[Y_1=y_1]} \cdot \frac{\Pr[X_2=x_2|W]\cdot\Pr[Y_2=y_2|W,X=(x_1,x_2)]}{\Pr[X_2=x_2]\cdot\Pr[Y_2=y_2]} \cdot \frac{C(x_1,x_2,y_1,y_1)}{Q(x_1,x_2,y_1,y_1)}$

Proving Lemma 15, cont.

Proving Lemma 15, cont.

$$
\begin{aligned}
D(C||U) = &\mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{\Pr\left[X_1 = x_1 | W\right] \cdot \Pr\left[Y_1 = y_1 | W, X = (x_1, x_2)\right]}{\Pr\left[X_1 = x_1\right] \cdot \Pr\left[Y_1 = y_1\right]}\right] \\
&+ \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{\Pr\left[X_2 = x_2 | W\right] \cdot \Pr\left[Y_2 = y_2 | W, X = (x_1, x_2)\right]}{\Pr\left[X_2 = x_2\right] \cdot \Pr\left[Y_2 = y_2\right]}\right] \\
&+ \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{C(x_1, x_2, y_1, y_2)}{Q(x_1, x_2, y_1, y_2)}\right].
\end{aligned}
$$

Proving Lemma 15, cont.

$$
\begin{aligned}
D(C||U) = & \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{\Pr\left[X_1 = x_1|W\right]\cdot \Pr\left[Y_1 = y_1|W, X = (x_1,x_2)\right]}{\Pr\left[X_1 = x_1\right]\cdot \Pr\left[Y_1 = y_1\right]}\right] \\
& + \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{\Pr\left[X_2 = x_2|W\right]\cdot \Pr\left[Y_2 = y_2|W, X = (x_1,x_2)\right]}{\Pr\left[X_2 = x_2\right]\cdot \Pr\left[Y_2 = y_2\right]}\right] \\
& + \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{C(x_1,x_2,y_1,y_2)}{Q(x_1,x_2,y_1,y_2)}\right].
\end{aligned}
$$

It follows that

$$
\begin{aligned}
D(C||U) = & D(X_1|_W, X_2|_{W,X_1}, Y_1|_{W,X}, Y_2|_{W,X,Y_1}||X_1, X_2|_{W,X_1}, Y_1, Y_2|_{W,X,Y_1}) \\
& + D(X_2|_W, X_1|_{W,X_2}, Y_2|_{W,X}, Y_1|_{W,X,Y_2}||X_2, X_1|_{W,X_2}, Y_2, Y_1|_{W,X,Y_2}) \\
& + D(C||Q),
\end{aligned}
$$

Proving Lemma 15, cont.

$$
\begin{aligned}
D(C||U) = & \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{\Pr[X_1 = x_1|W]\cdot \Pr[Y_1 = y_1|W, X = (x_1,x_2)]}{\Pr[X_1 = x_1]\cdot \Pr[Y_1 = y_1]}\right] \\
& + \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{\Pr[X_2 = x_2|W]\cdot \Pr[Y_2 = y_2|W, X = (x_1,x_2)]}{\Pr[X_2 = x_2]\cdot \Pr[Y_2 = y_2]}\right] \\
& + \mathop{\mathrm{E}}_{(x_1,x_2,y_1,y_2)\leftarrow C}\left[\log \frac{C(x_1,x_2,y_1,y_2)}{Q(x_1,x_2,y_1,y_2)}\right].
\end{aligned}
$$

It follows that

$$
\begin{aligned}
D(C||U) = & D(X_1|_W, X_2|_{W,X_1}, Y_1|_{W,X}, Y_2|_{W,X,Y_1} || X_1, X_2|_{W,X_1}, Y_1, Y_2|_{W,X,Y_1}) \\
& + D(X_2|_W, X_1|_{W,X_2}, Y_2|_{W,X}, Y_1|_{W,X,Y_2} || X_2, X_1|_{W,X_2}, Y_2, Y_1|_{W,X,Y_2}) \\
& + D(C||Q),
\end{aligned}
$$

and the proof follows since $D(\cdot||\cdot) \geq 0$. $\square$

Parallel repetition of interactive proofs

Parallel repetition of interactive proofs

- Similar proof to the public-coin proof we gave above.

Parallel repetition of interactive proofs

- Similar proof to the public-coin proof we gave above.
- In each round, the attacker $\widetilde{\mathsf{P}}$ samples random continuations of $(\widetilde{\mathsf{P}^{(k)}, \mathsf{V}^{(k)}})$, till he gets an accepting execution.

Parallel repetition of interactive proofs

- Similar proof to the public-coin proof we gave above.
- In each round, the attacker $\widetilde{\mathsf{P}}$ samples random continuations of $(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)})$, till he gets an accepting execution.
- Why fails us to extend this approach for non-public-coin interactive arguments?

Section 3

Parallel amplification for any interactive argument

Parallel amplification theorem for any protocol

Parallel amplification theorem for any protocol

- Can we amplify the security of any interactive argument “in parallel”?

Parallel amplification theorem for any protocol

- Can we amplify the security of any interactive argument “in parallel”?
- Yes we can!